Legal Ramifications of Cyberspace Attacks
Javi Antuña (39-2255)

The evolving cyber domain demands a modification of governing rules and regulations. The international community lacks cohesion when enforcing retaliatory attacks against state actors or punishment against non-state actors. Few states have incorporated lessons learned from the cyber attacks of Estonia, 2007 and Georgia, 2008. Although the just war principles of jus ad bellum and jus in bello govern retaliatory attacks against state actors, loop holes in the legal system arose when implementing force, proportionality, and discriminative actions. Non-state actors often escape criminal punishment for lack of intelligence and determination by states to impose consequences.

Law of armed conflict (LOAC) in the US attempts to balance two objectives when dealing in the cyberspace domain. The first is the ability of a sovereign state to protect itself from cyber attacks, and the second is the ability to protect innocent civilians from unnecessary suffering. LOAC integrates four components or principles to maintain stability between the two objectives and formulating counter attacks: principle of military necessity, principle of distinction, principle of proportionality, and principle of chivalry. The principle of military necessity is the ability of the military to take only the actions necessary to achieve their objectives. The principle of distinction requires a military commander to distinguish between combatants and civilians, while also necessitating the careful selection of targets and weapons to avoid collateral damage. The principle of proportionality demands an equal amount of retribution when conducting counter attacks, requiring a commander to consider secondary effects on civilian populations and non-combatants. Finally, the principle of chivalry requires adherence to the established rule of law by the international community.[1] These principles maintain a balance between the LOAC objectives of the US and the differences between societies, cultures, and warfare.

Problems with the rule of law in cyberspace are determining the source of the cyber attacks, what standards of retribution are justifiable during peacetime or wartime, and how will non-state actors be tried in criminal law. A key concern in the cyber domain is intelligence and determining where attacks originate. "Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."[2] With interconnected networks, the cyber world is composed of a wide variety of servers and hubs: military, commercial, private, and bogus registered sites. Understanding who planned the attack versus where the attack originated from is of particular difficulty, as was the case with the cyber attacks against Estonia in 2007 and Georgia in 2008. According to Arbor Networks and the Shadowserver Foundation, all attacks originated from global sources and at least six different command and control servers.[3] Some servers were for hire and others were used for extortion, further complicating the determination of the source.

Establishing whether the source of attack is the conduct of a private actor or state actor determines liability. "The governing principle of state responsibility under international law has been that the conduct of private actors – both entities and persons – is not attributable to the state, unless the state has directly and explicitly delegated a part of its tasks and functions to a private entity."[4] Two key questions must be answered: 1) has the person acted as an agent of a state; 2) whether his /her actions qualify as actions of the state. If both answers are yes, then the rules under international law apply, and the state is liable for the wrongful acts committed by the private sector. Keeping in mind the four principles of LOAC, the US is justifiable in conducting

counter attacks; however, determining whether the cyber attack was conducted during peacetime or wartime also governs the conduct of the US when planning retribution.

The standards governing the laws of applying force differ between jus ad bellum (peacetime) and jus in bello (wartime). Until recently, a quantitative approach for retribution made sense. Reciprocation for kinetic effects is logical; however, non-kinetic operations calls for different logic when formulating a counter attack. During jus ad bellum operations, international law under the United Nations Charter article 2 paragraph 4 states, "All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations."[5] Rather than reverting to force, the UN would prefer political, diplomatic, and economic pressures to diffuse aggression and prevent war. Using the last resort of force is a preferable approach; unfortunately, the severity, directness, and measurability of an attack have lasting impacts when considering retribution.[6] In Estonia, for example banks, telephone systems, and newspaper sites were affected. Although there were no casualties, the Estonian way of life suffered significantly and warranted a counter attack. Lack of an overarching governing law limited Estonia's retribution effort; furthermore, having a legitimate authority to conduct counter attacks would simplify circumstances two fold. First, it would validate retribution and UN laws would spell out actions available to conduct reprisal. Second, having authority to conduct reprisals may deter future cyber attacks from potential private and state actors. Peacetime operations require new penal codes and regulations within the international community to avoid escalation of hostilities when considering retaliation attacks. In addition, monetary and imprisonment consequences are viable opportunities to deter potential future attacks.

During jus in bello operations, two principles must be followed to ensure just war standards: discrimination and proportionality. When conducting cyber attacks, distinguishing lawful from unlawful targets is a difficult task. A principle under international law found in the Geneva Conventions states: "In order to ensure respect for and protection of the civilian population and between civilian objects, the Parties of the conflict shall at all times distinguish between the civilian population and combatants and civilian objects and military objectives and accordingly shall direct their operations only against military objectives."[7] Most military facilities support surrounding cities and infrastructures; therefore, the feasibility of attacking infrastructure or computer networks without affecting civilians is impractical. In addition, distinguishing between an electrical grid of an early warning radar from a banking infrastructure is extremely difficult. The risk of misidentifying a target increases exponentially when conducting cyber attacks. When planning retribution, the selection of tactics and weapons deserves extra attention. Secondary effects can have lasting impacts, and oftentimes lead to a violation with the principle of proportionality. "A lack of full knowledge as to what is being hit; the inability to surgically craft the amount of force being applied to the target; and the inability to ensure the weapons strike precisely the right point" all affect the commanders choice of retribution options.[8] Just as in peacetime operations, preventing escalation of hostilities and limiting collateral damage with the careful selection of weapons to distinguish lawful from unlawful targets is paramount.

Unfortunately, proving the support by any certain state to private sector has proven nearly impossible, as neither cyber attacks in Estonia nor Georgia have confirmed state sponsorship. If attribution cannot be classified as state sponsorship, then the private entity is held liable by national and international criminal law. As technology and the cyber domain evolve, few states

have incorporated provisions of computer crimes in their criminal law. The Cyber Crime Convention of Europe was the first international agreement to adopt procedures for investigating cyber crimes such as identity theft, intrusions into networks, and spread of viruses.[9] Unfortunately, the international community is slow to follow the European Convention, and often entails an actual cyber attack to establish penal codes. Estonia established article 207 of the penal code after their attack stating: "unlawful interference or hindrance of the operation of a computer system by way of entry, transmission, deletion, damaging, alteration or blocking of data is punishable by a pecuniary punishment or up to five years' imprisonment if significant damage is thereby caused or the operation of a computer system of a vital sector (critical infrastructure) or the provision of public services is thereby hindered."[10] Additionally, Georgia established three articles under their penal code stating "unlawful infiltration into the computer information (Art. 303), creating, applying and disseminating a program damaging computers (Art. 304), and infringement of the rules for exploiting computers, computer systems or their networks (Art. 305) is prohibited and punishable."[11] Both states address consequences to damaging or destroying computer networks, but leave many "grey areas" such as damages to infrastructures, monetary fallbacks if commercial systems are inoperable, and civilian casualties to name a few.

Given the lack of clear policies and penal codes in the international security environment, attacks by means of non-kinetic effects seem more attractive to an enemy via private entities. Initiating an investigation with lack of intelligence will yield poor results; furthermore, the absence of penal codes established in the international community results with fewer ramifications. From a legal point of view, the International Court Justice (ICJ) must include provisions to cyber crime attacks by establishing organizations to track, monitor, and investigate

cyber attacks. In addition, the court must include stricter monetary and penal punishments to deter future attacks from occurring. A good example of monetary punishment is Georgia in an Article stating "…punishable by a penalty to from 70 to 360 times the daily salary."[12] The international courts would do well by establishing a standard of punishable crimes for cyber attacks and their ramifications under penal codes. It will ensure the widest measure of assistance in civil proceedings by defining the characteristics of punishable crimes that threaten the security, order, sovereignty, or other essential interests of a state.

In the end, the surfacing of cyber attacks calls for the international community to set standards of reciprocity and/or punishment when countering cyber attacks. Intelligence must track and identify state actors. Cyber attacks by state actors can go no longer without retribution. Non-state actors necessitate consequences when orchestrating and conducting cyber attacks. The international community would do well by studying and incorporating lesson learned in the Estonian and Georgian cyber attacks. In particular, the justice system should incorporate monetary and imprisonment consequences to deter future cyber attacks. LOAC rules of the US also need to be applied to the governing rules of retaliatory attacks. The international community must come together and devise new laws and regulations to avoid a world of uncertainty when trying to impose ramifications for cyber attacks.

[1] WS-507 The Geneva Conventions and America's War on Terror, Nov 2009.
[2] Kramer, Franklin D., Starr Stuart H., Wentz Larry K., *Cyberpower and National Security*, 2009, xvi.
[3] Cyber attacks against Georgia: Legal Lessons Identified, Nov 2008, 12.
[4] Ibid., 21.
[5] Kramer, Franklin D., Starr Stuart H., Wentz Larry K., *Cyberpower and National Security*, 2009, 526.
[6] Ibid., 527-530.
[7] Ibid., 533-534.
[8] Ibid., 536.
[9] Cyber attacks against Georgia: Legal Lessons Identified, Nov 2008, 23.
[10] Ibid., 24.
[11] Ibid., 24.
[12] Ibid., 24.